

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

<p>Nicole Johnson, individually and on behalf of all others similarly situated,</p> <p style="text-align: center;"><i>Plaintiff,</i></p> <p>v.</p> <p>Consulting Radiologists, Ltd.,</p> <p style="text-align: center;"><i>Defendant.</i></p>	<p>Case No.: _____</p> <p>CLASS ACTION COMPLAINT</p> <p>JURY DEMAND</p>
---	--

Plaintiff Nicole Johnson (“Plaintiff”), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against Defendant Consulting Radiologists, Ltd. (“Consulting Radiologists, Ltd.” or “Defendant”), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Data Breaches have become entirely too common, and the reason is the lack of attention and resources that companies like the Defendant expend on protecting sensitive information.

2. Plaintiff brings this class action against Consulting Radiologists, Ltd. for its failure to properly secure Plaintiff and Class Members’ personally identifiable information (“PII”) and personal health information (“PHI”). According to Defendant, Consulting

Radiologists, Ltd., the PII and PHI may have included patients' names, addresses, dates of birth, Social Security numbers, health insurance information, medical information.¹

3. Consulting Radiologists, Ltd. failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiff seeks, among other things, orders requiring Consulting Radiologists, Ltd. to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

4. The Private Information compromised in the Data Breach included personal identifiable information of individuals whose Private Information was maintained by Defendant, including Plaintiff.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was hired to protect.

6. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

7. Upon information and belief, Defendant breached its duties and obligations

¹ Notice of Data Privacy Event, Consulting Radiologists, Ltd., <https://www.consultingradiologists.com/notice-of-data-privacy-event/> (last visited June 21, 2024).

by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

9. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals

a period of unimpeded access to the Private Information of Plaintiff and Class Members.

10. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

12. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the Dark Web.

13. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

14. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred

mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of implied contract, (iii) breach of fiduciary duty (iv) unjust enrichment.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

18. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

19. Defendant, Consulting Radiologists, Ltd., was formed in Minnesota, with its principal place of business at 7505 Metro Blvd Ste 400, Edina, Minnesota, 55439.

20. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

21. Plaintiff Nicole Johnson is an adult individual who at all relevant times has been a citizen and resident of Minnesota, who has been a patient at Consulting Radiologists, Ltd. in recent years. She gave PII and PHI to Consulting Radiologists, Ltd. as a condition of receiving medical services.

22. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing their Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

23. Plaintiff is not aware of ever being part of a data breach involving her PII or PHI and is concerned that it and other private information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including checking her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

24. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual

or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

25. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

26. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

28. This Court has personal jurisdiction over Defendant because it is a Minnesota corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover,

Defendant is domiciled in this District, maintains Plaintiff and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

The Data Breach

30. On February 12, 2024, Defendant became aware of suspicious activity in its "network environment"².

31. On April 17, 2024, Defendant identified affected persons and yet still waited two months to notify them.

32. Consulting Radiologists, Ltd.'s disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what Consulting Radiologists, Ltd. knows about the degree to which the data has been disseminated.

33. Consulting Radiologists, Ltd. has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, Consulting Radiologists, Ltd. has taken to secure the PII and PHI still in its

² Notice of Data Privacy Event, Consulting Radiologists, Ltd., <https://www.consultingradiologists.com/notice-of-data-privacy-event/> (last visited June 21, 2024).

possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff and Class Members' interests, and ensure that Consulting Radiologists, Ltd. has proper measures in place to prevent similar incidents from occurring in the future.

The Healthcare Sector Is a Primary Target for Data Breaches

34. Consulting Radiologists, Ltd. was on notice that companies in the healthcare industry are susceptible targets for data breaches.

35. Consulting Radiologists, Ltd. was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."³

³ Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf>) (last accessed Mar. 14, 2023).

36. The number of reported North American data breaches increased by over 50 percent in 2021, from 1,080 in 2020⁴, to 1,638 in 2021.⁵ As a recent report reflects, “[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns.”⁶

37. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors, and it had the highest rate of exposure for each breach.⁷ Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁸ Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their

⁴ See Verizon 2021 Data Breach Investigations Report, at 97, <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf> (last accessed Mar. 14, 2023).

⁵ See Verizon 2022 Data Breach Investigations Report, at 83 (available at <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>) (last accessed Mar. 14, 2023).

⁶ *Id.* at 62.

⁷ 2018 *End-of-Year Data Breach Report*, Identity Theft Resource Center (available at <https://www.idtheftcenter.org/2018-data-breaches>) (last accessed Mar. 14, 2023).

⁸ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>) (last accessed Mar. 14, 2023).

identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.⁹

38. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by “bad actors” such as cybercriminals.¹⁰ “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹¹

39. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

⁹ *Id.*

¹⁰ 2019 HIMSS Cybersecurity Survey (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

¹¹ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks>) (last accessed Mar. 14, 2023).

threaten the privacy and security of patients' health and financial information, but also patient access to care.¹²

40. As a major healthcare provider, Consulting Radiologists, Ltd. knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Consulting Radiologists, Ltd. patients because of a breach. Consulting Radiologists, Ltd. failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Consulting Radiologists, Ltd. Stores Plaintiff and Class Members' PII and PHI

41. Consulting Radiologists, Ltd. obtains and stores a massive amount of its patients' PII and PHI. As a condition of engaging in health services, Consulting Radiologists, Ltd. requires that patients entrust it with highly confidential PII and PHI.

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII and PHI, Consulting Radiologists, Ltd. assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and, as Consulting Radiologists, Ltd.'s current and former patients, they rely on Consulting Radiologists, Ltd. to keep this information

¹² Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019) (available at <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>) (last visited Mar. 14, 2023).

confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI Are Valuable and Subject to Unauthorized Disclosure

44. Consulting Radiologists, Ltd. was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

45. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.¹³ Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the “dark web.” PHI can sell for as much as \$363 on the dark web, according to the Infosec Institute.¹⁴

46. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim’s medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

47. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim’s PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. “Medical identity theft is a

¹³ Federal Trade Commission, What To Know About Identity Theft (available at <https://consumer.ftc.gov/articles/what-know-about-identity-theft>) (last accessed Mar. 14, 2023).

¹⁴ Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/>) (last accessed Mar. 14, 2023).

growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁵

48. The ramifications of Consulting Radiologists, Ltd.’s failure to keep its patients’ PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

49. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

50. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.¹⁶ This gives thieves ample time to seek multiple treatments under the victim’s name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.¹⁷

¹⁵ Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at <https://khn.org/news/rise-of-identity-theft/>) (last accessed Mar. 14, 2023).

¹⁶ See Medical ID Theft Checklist (available at <https://www.identityforce.com/blog/medical-id-theft-checklist-2>) (last accessed Mar. 14, 2023).

¹⁷ Experian, The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches (available at <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>) (last accessed Mar. 14, 2023).

51. Consulting Radiologists, Ltd. knew, or should have known, the importance of safeguarding its patients' PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Consulting Radiologists, Ltd. patients because of a breach. Consulting Radiologists, Ltd. failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

**The Data Breach Exposed Plaintiff and Class Members
to Identity Theft and Out-of-Pocket Losses**

52. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

53. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, Consulting Radiologists, Ltd.'s policies and practices with respect to maintaining the security of its patients' PII and PHI were reckless, or at the very least, negligent.

54. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be compensated for the time they have expended because of Consulting Radiologists, Ltd.'s misfeasance.

55. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.¹⁸

56. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- a. losing the inherent value of their PII and PHI;
- b. identity theft and fraud resulting from the theft of their PII and PHI;
- c. costs associated with the detection and prevention of identity theft;
- d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;
- e. lowered credit scores resulting from credit inquiries following fraudulent activities;
- f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection

¹⁸ 2014 LexisNexis True Cost of Fraud Study (available at <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>) (last accessed Mar. 14, 2023).

services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

Consulting Radiologists, Ltd.’s Lax Security Violates HIPAA

57. Consulting Radiologists, Ltd. had a non-delegable duty to ensure that all PHI it collected and stored was secure.

58. Consulting Radiologists, Ltd. is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

59. These rules establish national standards for the protection of patient information, including protected health information, defined as “individually identifiable health information” which either “identifies the individual” or where there is a “reasonable basis to believe the information can be used to identify the individual,” that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

60. HIPAA limits the permissible uses of “protected health information” and prohibits unauthorized disclosures of “protected health information.”

61. HIPAA requires that Consulting Radiologists, Ltd. implement appropriate safeguards for this information.

62. Despite these requirements, Consulting Radiologists, Ltd. failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, Consulting Radiologists, Ltd. failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

63. Consulting Radiologists, Ltd. failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff and Class Members' PHI.

Consulting Radiologists, Ltd. Violated FTC Guidelines

64. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited Consulting Radiologists, Ltd. from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' PII is an "unfair practice" in violation of the FTC Act. *See, e.g., Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹⁹

¹⁹ Federal Trade Commission, *Start With Security: A Guide for Business* (available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>) (last accessed Mar. 14, 2023).

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.²⁰ The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.²¹

68. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Consulting Radiologists, Ltd. failed to properly implement basic data security practices. Consulting Radiologists, Ltd.'s failure to employ reasonable and

²⁰ Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

²¹ FTC, *Start With Security*, *supra* 19.

appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Consulting Radiologists, Ltd. was at all times fully aware of its obligation to protect its patients' PII and PHI because of its position as a healthcare provider. Consulting Radiologists, Ltd. was also aware of the significant repercussions that would result from its failure to do so.

CLASS ALLEGATIONS

71. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

Nationwide Class: All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach disclosed on April 2, 2024.

Minnesota Class: All residents of the state of Minnesota whose Private Information was compromised in the Defendant's Data Breach disclosed on April 2, 2024.

72. The Nationwide Class and Minnesota Class are referred to collectively herein as the "Class." Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

73. Plaintiff reserves the right to modify or amend these definitions of the proposed classes prior to moving for class certification.

74. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. Consulting Radiologists, Ltd. has disclosed that the Data Breach affected approximately 827,149 patients.

75. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Class Members;
- b. Whether Defendant was negligent in collecting and storing Plaintiff and Class Members' PII and PHI;
- c. Whether Defendant had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;
- d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff and Class Members' PII and PHI;
- e. Whether Defendant failed to adequately safeguard the PII and PHI of Class Members;
- f. Whether Defendant failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;
- g. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

- h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of Defendant's wrongful conduct;
- i. Whether Plaintiff and Class Members are entitled to restitution because of Defendant's wrongful conduct;
- j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and
- k. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

76. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff PII and PHI, like that of every other Class Member, was disclosed by Consulting Radiologists, Ltd.. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiff is advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

77. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Consulting Radiologists, Ltd. to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

78. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Consulting Radiologists, Ltd. has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Consulting Radiologists, Ltd.'s policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Consulting Radiologists, Ltd.'s conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

79. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Consulting Radiologists, Ltd.. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

80. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and

appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Consulting Radiologists, Ltd. would necessarily gain an unconscionable advantage in non-class litigation, since Consulting Radiologists, Ltd. would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

81. The litigation of Plaintiff's claims is manageable. Consulting Radiologists, Ltd.'s uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

82. Adequate notice can be given to Class Members directly using information maintained in Consulting Radiologists, Ltd.'s records.

83. Unless a class-wide injunction is issued, Consulting Radiologists, Ltd. may continue to maintain inadequate security with respect to the PII and PHI of Class Members, Consulting Radiologists, Ltd. may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Consulting Radiologists, Ltd. may continue to act unlawfully as set forth in this Complaint.

COUNT I
NEGLIGENCE

**(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)**

84. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

85. Consulting Radiologists, Ltd. knowingly collected, came into possession of, and maintained Plaintiff and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing Consulting Radiologists, Ltd.'s security protocols to ensure that Plaintiff and Class Members' Private Information in Defendant's possession was adequately secured and protected, that Plaintiff and Class Members' Private Information on Consulting Radiologists, Ltd.'s networks were not accessible to criminals without authorization, and that Consulting Radiologists, Ltd. employees tasked with maintaining such information were adequately trained on security measures regarding the security of customers/patients' PII and PHI.

86. As a condition of utilizing Consulting Radiologists, Ltd.'s services, Plaintiff and Class Members were obligated to provide their PII and PHI to Consulting Radiologists, Ltd..

87. Plaintiff and Class Members entrusted their PII and PHI to Consulting Radiologists, Ltd. with the understanding that Consulting Radiologists, Ltd. would

safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

88. Consulting Radiologists, Ltd. knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiff and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

89. Consulting Radiologists, Ltd. also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and Class Members' PII and PHI.

90. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape, including the explosion of data breaches involving similarly situated healthcare providers.

91. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Consulting Radiologists, Ltd. knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the critical importance of providing adequate security of that information, the necessity for encrypting PHI stored on Consulting Radiologists, Ltd.'s systems, and that it had inadequate IT security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

92. Consulting Radiologists, Ltd.'s own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Consulting Radiologists, Ltd.'s misconduct included,

but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

93. Plaintiff and Class Members had no ability to protect their PII and PHI that was in Consulting Radiologists, Ltd.'s possession.

94. Consulting Radiologists, Ltd. was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

95. Consulting Radiologists, Ltd. had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

96. Consulting Radiologists, Ltd. had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

97. Consulting Radiologists, Ltd. systematically failed to provide adequate security for data in its possession.

98. Consulting Radiologists, Ltd., through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within its possession.

99. Consulting Radiologists, Ltd., through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII and PHI.

100. Consulting Radiologists, Ltd., through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII and PHI within Consulting Radiologists, Ltd.'s possession might have been compromised and precisely the type of information compromised.

101. Consulting Radiologists, Ltd. breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

102. But for all of Consulting Radiologists, Ltd.'s acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiff's and Class Members' PII and PHI would not have been compromised.

103. Plaintiff never transmitted her own unencrypted PHI over the internet or any other unsecured source.

104. Following the Data Breach, Plaintiff's PHI has been seized by unauthorized third parties who are now free to exploit and misuse that PHI without any ability for Plaintiff to recapture and erase that PHI from further dissemination—Plaintiff's PHI is forever compromised.

105. But for the Data Breach, Plaintiff would not have incurred the loss and publication of her PHI and other injuries.

106. There is a close causal connection between Consulting Radiologists, Ltd.'s failure to implement security measures to protect Plaintiff's and Class Members' PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' PHI was accessed and compromised as the proximate result of Consulting Radiologists, Ltd.'s failure to exercise reasonable care in

safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures and encryption.

107. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

108. As a result of Consulting Radiologists, Ltd.'s negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes.

109. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

110. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Consulting Radiologists, Ltd. to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Consulting Radiologists, Ltd. to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE PER SE
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

111. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

112. Pursuant to the HIPAA (42 U.S.C. § 1302d et seq.), the FTC Act, Consulting Radiologists, Ltd. was required by law to maintain adequate and reasonable data and

cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' PHI and PII.

113. Consulting Radiologists, Ltd. breached its duties by failing to employ industry standard data and cybersecurity measures to ensure its compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

114. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Consulting Radiologists, Ltd. networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII and PHI.

115. Plaintiff's and Class Members' PII and PHI constitute personal property that was stolen due to Consulting Radiologists, Ltd.'s negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

116. Consulting Radiologists, Ltd.'s conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted PII and PHI, and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Consulting Radiologists, Ltd.'s conduct. Plaintiff and Class Members seek damages and other relief as a result of Consulting Radiologists, Ltd.'s negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

117. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

118. When Plaintiff and Class Members provided their PII and PHI to Consulting Radiologists, Ltd. they entered into implied contracts with Consulting Radiologists, Ltd., under which Consulting Radiologists, Ltd. agreed to take reasonable steps to protect Plaintiff and Class Members' PII and PHI, comply with its statutory and common law duties to protect Plaintiff and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

119. Consulting Radiologists, Ltd. solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of provision of healthcare services. Plaintiff and Class Members accepted Consulting Radiologists, Ltd.'s offers and provided their PII and PHI to Consulting Radiologists, Ltd..

120. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Consulting Radiologists, Ltd.'s data security practices complied with its statutory and common law duties to adequately protect Plaintiff and Class Members' PII and PHI and to timely notify them in the event of a data breach.

121. Plaintiff and Class Members paid money to Consulting Radiologists, Ltd. to receive healthcare services. Plaintiff and Class Members reasonably believed and expected

that Consulting Radiologists, Ltd. would use part of those funds to obtain adequate data security. Consulting Radiologists, Ltd. failed to do so.

122. Plaintiff and Class Members would not have provided their PII and PHI to Consulting Radiologists, Ltd. had they known that they would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

123. Plaintiff and Class Members fully performed their obligations under their implied contracts with Consulting Radiologists, Ltd..

124. Consulting Radiologists, Ltd. breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

125. The losses and damages Plaintiff sustained, include, but are not limited to:

- a. Theft of her PII and PHI;
- b. Costs associated with purchasing credit monitoring and identity theft protection services;
- c. Costs associated with the detection and prevention of identity theft and unauthorized use of her PII and PHI;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling, and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by her Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of her Private Information entrusted, directly or indirectly, to Consulting Radiologists, Ltd. with the mutual understanding that Consulting Radiologists, Ltd. would safeguard Plaintiff and Class Members' data against theft and not allow access and misuse of her data by others;

h. Continued risk of exposure to hackers and thieves of her Private Information, which remains in Consulting Radiologists, Ltd.'s possession and is subject to further breaches so long as Consulting Radiologists, Ltd. fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

126. As a direct and proximate result of Consulting Radiologists, Ltd.'s breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
BREACH OF FIDUCIARY DUTY
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

127. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

128. Consulting Radiologists, Ltd. has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship, as a consequence of the special relationship of trust and confidence that exists between patients (like Plaintiff and Class Members) and their medical care providers (like Consulting Radiologists, Ltd.).

129. In light of their special relationship, Consulting Radiologists, Ltd. has become the guardian of Plaintiff's and Class Members' PII and PHI. Consulting Radiologists, Ltd. has become a fiduciary, created by its undertaking and guardianship of patient PII and PHI, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

130. Consulting Radiologists, Ltd. breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

- a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' PII and PHI;
- b. timely notify and/or warn Plaintiff and Class Members of the Data Breach;

- c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);
- f. identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- g. protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);
- h. protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- i. ensure its compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);
- j. properly use and disclose PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

- k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);
- l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c); and
- m. otherwise failing to safeguard Plaintiff and Class Members' Personal Information.

131. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect patient Personal Information in its continued

possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

132. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
UNJUST ENRICHMENT
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

133. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

134. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by Consulting Radiologists, Ltd. and that was stolen in the Data Breach.

135. Consulting Radiologists, Ltd. benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. Consulting Radiologists, Ltd. understood that it so benefitted.

136. Consulting Radiologists, Ltd. also understood and appreciated that Plaintiff's and Class Members' PHI and PII was private and confidential and that its value depended upon Consulting Radiologists, Ltd. maintaining its privacy and confidentiality.

137. But for Consulting Radiologists, Ltd.'s willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with Consulting Radiologists, Ltd.. Further, if Consulting Radiologists,

Ltd. had disclosed that its data security measures were inadequate, Consulting Radiologists, Ltd. would not have been permitted to continue in operation by regulators and the healthcare marketplace.

138. As a result of Consulting Radiologists, Ltd.'s wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII), Consulting Radiologists, Ltd. has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

139. Consulting Radiologists, Ltd.'s unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

140. Under the common law doctrine of unjust enrichment, it is inequitable for Consulting Radiologists, Ltd. to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PHI and PII in an unfair and unconscionable manner. Consulting Radiologists, Ltd.'s retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

141. The benefit conferred upon, received, and enjoyed by Consulting Radiologists, Ltd. was not conferred officiously or gratuitously, and it would be inequitable and unjust for Consulting Radiologists, Ltd. to retain the benefit.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

142. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

143. Consulting Radiologists, Ltd. owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

144. Consulting Radiologists, Ltd. still stores Plaintiff's and Class Members' PII and PHI.

145. Since the Data Breach, Consulting Radiologists, Ltd. has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

146. Consulting Radiologists, Ltd. has not satisfied its legal duties to Plaintiff and Class Members.

147. Actual harm has arisen in the wake of the Data Breach regarding Consulting Radiologists, Ltd.'s duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and Consulting Radiologists, Ltd.'s failure to address the security failings that led to that exposure.

148. Plaintiff, therefore, seeks a declaration: (a) that Consulting Radiologists, Ltd. existing security measures do not comply with its duties of care to provide adequate

security; and (b) that to comply with its duties of care, Consulting Radiologists, Ltd. must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. ordering that Consulting Radiologists, Ltd. engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Consulting Radiologists, Ltd.'s systems on a periodic basis, and ordering Consulting Radiologists, Ltd. to promptly correct any problems or issues detected by such third-party security auditors;
- b. ordering that Consulting Radiologists, Ltd. engage third-party security auditors and internal personnel to run automated security monitoring;
- c. ordering that Consulting Radiologists, Ltd. audit, test, and train its security personnel regarding any new or modified procedures;
- d. ordering that Consulting Radiologists, Ltd. segment patient data by, among other things, creating firewalls and access controls so that if one area of Consulting Radiologists, Ltd.'s system is compromised, hackers cannot gain access to other portions of Consulting Radiologists, Ltd. systems;
- e. ordering that Consulting Radiologists, Ltd. purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provision of services;
- f. ordering that Consulting Radiologists, Ltd. conduct regular computer system scanning and security checks;

g. ordering that Consulting Radiologists, Ltd. routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Consulting Radiologists, Ltd. to meaningfully educate its current, former, and prospective patients about the threats they face because of the loss of their PHI to third parties, as well as the steps they must take to protect themselves.

COUNT VII
VIOLATION OF MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)

149. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

150. Defendant, Plaintiff, and Class members are each a “person” as defined by Minn. Stat. § 325F.68(3).

151. Defendant’s goods, services, commodities, and intangibles are “merchandise” as defined by Minn. Stat. § 325F.68(2).

152. Defendant engaged in “sales” as defined by Minn. Stat. § 325F.68(4).

153. Defendant engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of services, in violation of Minn. Stat. § 325F.69(1), including omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff’s and Class members’ PII and PHI.

154. The Minnesota Consumer Fraud Act [MCFA] prohibits “[t]he act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoined as provided in section 325F.70.” Minn. Stat. § 325F.69, subd. 1.

155. Minn. Stat. §8.31, subds. 1 and 3a allows any person injured by a violation of Minn. Stat. § 325F.69 to bring a civil action to recover damages, together with costs and disbursements, including reasonable attorney's fees, and to receive other equitable relief as determined by the court.

156. Defendant engaged in deceptive practices by failing to disclose to Plaintiff and the Class that its data security measures were inadequate to protect their sensitive information.

157. Defendant represented, directly or indirectly, that it maintained appropriate safeguards to protect the personal and medical information of its patients. These representations were false, misleading, and deceptive.

158. Defendant failed to inform Plaintiff and the Class about its deficient data security practices, which constitutes a material omission.

159. Defendant intended that Plaintiff and the Class would rely on its representations and omissions regarding the secure of their personal and medical information.

160. Plaintiff and the Class reasonably relied on Defendant's representations and omissions, believing that their sensitive information was secure.

161. Defendant's deceptive acts and omissions directly caused the exposure of Plaintiff's and the Class's sensitive information in the Data Breach. As a direct and proximate result of the Defendant's deceptive practices, Plaintiff and the Class suffered injuries, including the risk of identity theft, economic losses, loss of privacy, and the need for ongoing credit monitoring and identity theft services.

162. Plaintiff and the Class incurred actual damages due to the exposure of their sensitive information, including but not limited to costs associated with credit monitoring and identity theft protection, economic losses from unauthorized use of their information, and emotional distress. Plaintiff and the Class are entitled to recover statutory damages under Minn. Stat. § 8.31, subd. 3a, due to Defendant's violation of Minn. Stat. § 325F.69.

Plaintiff and the Class seek injunctive relief requiring Defendant to implement and maintain reasonable security measures to protect the sensitive information of its patients, to undergo periodic security audits, and to provide appropriate credit monitoring and identity theft protection services to affected individuals.

COUNT VIII

**Purpose and Requirements of the Minnesota Health Records Act (MHRA)
(on behalf of Plaintiff and the Nationwide Class or,
in the alternative, the Minnesota Class)**

163. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

164. The Minnesota Health Records Act (MHRA), Minn. Stat. § 144.291 et seq., is designed to protect the confidentiality, integrity, and security of patients' health records. The Act establishes standards for the handling, access, and disclosure of health records by healthcare providers in Minnesota.

165. Consulting Radiologists, Ltd. is a "Patient Information Service" as defined by Minn. Stat. § 144.291(Sub-2)(h), a "Provider" as defined by Minn. Stat. § 144.291(Sub-2)(i), and/or a "Related Health Care Entity" as defined by Minn. Stat. § 144.291(Sub-2)(k).

166. Plaintiff and Class members are "Patients" as defined by Minn. Stat. § 144.291(Sub-2)(g).

167. The Plaintiff's and Class members' PHI that was the subject of the Data Breach included "Health Records" as defined by Minn. Stat. § 144.291(Sub-2)(c).

168. The Plaintiff's and Class members' PHI that was the subject of the Data Breach included "Identifying Information" as defined by Minn. Stat. § 144.291(Sub-2)(d).

169. The Plaintiff's and Class Members' Personal and Medical Information that was the subject of the Data Breach included information in an "Individually Identifiable Form" as defined by Minn. Stat. § 144.291(Sub-2)(e).

170. Minn. Stat. §8.31, subds. 1 and 3a, allow any person injured by a law "respecting unfair, discriminatory, and other unlawful practices in business, commerce, or trade" that the Attorney General may investigate and enforce, to bring a civil action to recover damages, together with costs and disbursements, including reasonable attorney's fees, and to receive other equitable relief as determined by the court.

171. Under the MHRA, patients have the right to expect that their health records will be maintained confidentially and securely. This includes rights to access their own health records, receive copies upon request, and be informed about how their health information is used and disclosed.

172. The MHRA requires healthcare providers to adopt administrative, technical, and physical safeguards to ensure the security and confidentiality of health records. This includes protecting against unauthorized access, use, or disclosure of patient information.

173. Although the MHRA does not explicitly require breach notification, it is generally understood that protecting the confidentiality and integrity of health records includes promptly addressing any security incidents or breaches.

174. Compliance with the MHRA is essential for healthcare providers to avoid regulatory penalties and to ensure the trust and confidence of their patients. Violations of the MHRA can result in administrative actions by regulatory bodies. Consulting Radiologists, Ltd., as a healthcare provider, had a statutory duty under the MHRA to protect the PHI of Plaintiff and the Class by implementing appropriate security measures. This duty is aligned with the general duty of care owed to patients to safeguard their personal and medical information.

175. By failing to secure its network and allowing unauthorized access to the health records of approximately 512,000 patients, Consulting Radiologists, Ltd. breached its duty of care. This breach is evidenced by the violation of the MHRA's requirements for data security and confidentiality.

176. The breach of duty directly resulted in the exposure of Plaintiff's and the Class's sensitive information. This exposure has caused and will continue to cause harm, including the risk of identity theft, economic losses, and the loss of privacy. The violation of the MHRA serves as compelling evidence of Consulting Radiologists' negligence in failing to protect patient health records.

177. The MCFA prohibits deceptive practices in connection with the sale of merchandise, which includes services. Consulting Radiologist's representations regarding the security of patient information and its failure to disclose the inadequate security measures constitute deceptive practices.

178. The occurrence of Data Breach, and resulting violation of the MHRA, demonstrates that Consulting Radiologist's security measures were not compliant with statutory requirements; thus, Consulting Radiologist engaged in deceptive practices by misrepresenting the adequacy of its data security measures to patients.

179. Plaintiff and the Class relied on Consulting Radiologist's representations about the security of their health information, believing it to be adequately protected. The violation of the MHRA and subsequent data breach have caused harm to Plaintiff and the Class, including economic losses and the need for credit monitoring and identity theft protection.

180. In violation of the MHRA, Consulting Radiologists, Ltd. released Health Records (i.e., their PHI), as defined by the MHRA, of Plaintiff and Class members without first obtaining consent or authorization.

181. In violation of the MHRA, Consulting Radiologists, Ltd. negligently or intentionally released Health Records (i.e., their PHI) of Plaintiff and Class members.

182. As a direct and proximate result of Consulting Radiologists, Ltd.'s violation of Minn. Stat. §144.291 et seq., Plaintiff and Class member now face an increased risk of future harm.

183. As a direct and proximate result of Consulting Radiologists, Ltd.'s violation of Minn. Stat. §144.291 et seq., Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

184. The violation of the MHRA by Consulting Radiologists, Ltd.'s supports the claims under the Minnesota Consumer Fraud Act. Plaintiff and the Class are entitled to damages and equitable relief due to Consulting Radiologists, Ltd.'s failure to comply with its statutory obligations to protect patient health records.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

- a. for an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;
- b. for equitable relief enjoining Consulting Radiologists, Ltd. - from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to

- issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- c. for equitable relief compelling Consulting Radiologists, Ltd. to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;
 - d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;
 - e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by Minn. Stat. 8.31, subd. 3a;
 - f. for prejudgment interest on all amounts awarded; and
 - g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 28, 2024

Respectfully submitted,

/s/ E. Michelle Drake

E. Michelle Drake, Bar No. 0387366
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T. 612.594.5999
F. 612.584.4470
emdrake@bm.net

**THE CONSUMER PROTECTION
FIRM, PLLC**

William “Billy” Peerce Howard
Florida Bar No.: 0103330
Amanda J. Allen, Esquire
Florida Bar No.: 0098228
401 East Jackson Street, Suite 2340
Truist Place
Tampa, FL 33602
(813) 500-1500
Billy@TheConsumerProtectionFirm.com
Amanda@TheConsumerProtectionFirm.com

*Attorneys for Plaintiff and the Proposed
Class*